2132/Image

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	]	ASGHARI-KAMRANI ET AL
Title	]	CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD
Application No.	]	09/940,635 ✓
Filed	]	Aug. 29, 2001
Examiner	]	Abdulhakim Nobahar
Supervisor	]	Gilberto Barron
Action Mail Date	]	02/07/2005
Response Date	]	04/27/2005

ARGUMENTS AND REMARKS IN RESPONSE TO OFFICE ACTION

Commissioner of Patents
Alexandria, V.A. 22313

Dear Sirs:

In response to the outstanding Office Action mailed on 02/07/2005, please consider the following remarks relative to the various documents cited on the "*Notice of References*" sheet.

BACKGROUND

Fraud and Identity theft, the taking of a person's identity for the purpose of committing a criminal act, is a growing national concern, both in terms of its affect on its victims, and its potential national security implications. Checking account fraud costs US banks USD 698 million in 2002, according to the American Bankers' Association, while those perpetrating the fraud attempted to take USD 4.3 billion in total. Identity theft costs financial institutions USD 47.6 billion in 2002-2003. A report issued in September 2003 by the Federal Trade Commission estimates that almost 10 million Americans were victims of some type of identity theft within the previous year.

Online Fraud and Identity theft happens because financial institutions and businesses do not have any solution to authenticate the customers' identity. Online businesses such as retailers assume that the person shopping online is the same person whose personal or financial information are given. Creditors assume that the person filling the application is the same person whose name and personal information are used in the application, unless there is clear evidence to the contrary. A business "authenticates" a customer by matching personal and financial information provided, such as name, SSN, birth date, etc., with information contained in third party databases (indirect authentication). If there is a match on at least a few items of information, it is assumed that the person is the same person who he says he is. This assumption itself is a direct result of a belief that sensitive personal and financial information can be kept secret and out of the hands of thieves. Yet the widespread incidence of fraud and identity theft, as detailed by the personal stories of its many victims, clearly demonstrates that this notion is false.

For authentication of users/customers, businesses are facing two different authentication problems:

Authentication Problem 1: The user/customer has an existing relationship with the enterprise/business and the business needs an authentication method to authenticate its users/customers. A good example would be a financial institution and its customers or a company and its employees. The enterprise/business may use one of these three different authentication methods or the combination of these to authenticate its users/customers:

a) Something the user/customer knows: like password
b) Something the user/customer owns: like smart card, tokens or IC card or software installation on user's computer
c) Something the user/customer is: Biometric information such as a fingerprint

Authentication Problem 2: The user/customer does not have an existing relationship with the enterprise/business. A good example would be an online retailer or an online auction site or an online creditor and new customers purchasing goods or services. In this situation, where customers can buy goods and services without having a prior relationship with that business, businesses do not have any solution to perform

user/customer authentication. The authentication methods ("a", "b", "c") mentioned above are not applicable here. Therefore, businesses are using third party databases to verify users/customers information such as name, address. But this type of authentication is not a foot proof that the user/customer is who he says he is (user's or customer's information is verified and not the identity of the user/customer). Therefore fraud and identity theft are dramatically increasing.

The present invention (Asghari-Kamrani et al, application 09/940,635) is a solution for ***Authentication Problem 2***. The present invention allows online businesses ("External-Entity") to directly authenticate their customers over the Internet using trusted authenticators ("Central-Entity") without having prior relationships with customers/users.

The patents mentioned on the "*Notice of References Cited*" sheet are intended to solve different problems than our invention. Therefore, there are no correlations between what those patents are solving and what the current invention is suggesting to solve.

IN COMPARISON WITH HARIF, SHLOMI (US-2002/0087881 A1)

The patent of Harif et al. is tackling a different problem, which is identifying and binding a process. A network server receives and analyzes a request for process execution associated with a task and packages the request so that the task may be completed. An embodiment of the system includes a network client that provides a request for process execution to a network server. The network server evaluates the request, and if acceptable, creates a process to be executed on a network host to complete the task.

The patent of Asghari-Kamrani et al (application 09/940,635) is for identification of users over a communication network such as Internet to answer the "Authentication Problem 2" and not for identifying and binding a process.

IN COMPARISON WITH MATSUMOTO, TSUTOMU ET AL (US-2002/0066042 A1)

The patent of Matsumoto et al, is also attempting to solve a different problem, which is a card settlement method. A mobile information terminal provided with an IC card read/write function and a wireless communication function for the settlement of a transaction in a business establishment. An *IC card* is used for authentication of the customer. So, the authentication method is hardware dependent (method "b" mentioned above).

The patent of Asghari-Kamrani et al (application 09/940,635) is solving the identification and authentication issues at the e-commerce level ("Authentication Problem 2"). This invention relates to a system that solves the e-commerce security and privacy issues and has nothing to do with a card settlement system. Our invention does no require user/customer to install any hardware device like an IC card for authentication.

IN COMPARISON WITH NENDELL ET AL (US-6,343,361 B1)

Nendell et al. is suggesting to solve "*Authentication problem 1*" by identifying the recipient communication device, such as a computer. A primary key generated from a master key is stored at a sending device and the recipient device. Based on the primary key, the sending device generates a passphrase and an associated secondary key, which includes an encrypted form of the recreation process the passphrase. The secondary key is transmitted to the recipient device, which can reconstruct the passphrase by decrypting the secondary key using the primary key. By reconstructing the passphrase, the secondary key verifies that it has used the correct primary key. The identity of a user of a communication device can be verified and authenticated, as well. The user is issued an authorization key, a copy of which is stored at a remote communication device with respect to the user. Using the authorization code, the user selects specified character positions of the passphrase and enters the resulting input code to the local communication device. The input code is transmitted to the remote communication device. Entering the appropriate input code verifies that the user possesses the authorization code.

Nendell is suggesting to store a primary key at the sending device (client) and the recipient device (server). Therefore, this authentication method is useful within an enterprise to solve "Authentication Problem 1" and is not applicable in e-commerce ("Authentication Problem 2").

The patent of Asghari-Kamrani et al (application 09/940,635) is solving the identification and authentication issues at the e-commerce level (*"Authentication Problem 2"*) and does not require to store any key in user's device for authentication.

IN COMPARISON WITH YU ET AL (US-6,067,621 A)

The patent of Yu et al, is a user authentication system for authenticating an authorized user of an IC card. This is again a solution to the "Authentication Problem 1" using authentication method "b" as mentioned above. A user authentication system for authenticating a user using an **IC card** in conjunction with a portable terminal used to generate a one-time password and a server used to generate a corresponding one-time password for user authentication. The IC card contains a secret key for generating a one-time password and predetermined random numbers. The portable terminal contains a card receiver for receiving the IC card, a random number memory for reading and storing, and then deleting the random numbers of the IC card, a first password generator for generating a one-time password by the secret key of the IC card and the random number, a first random number changer for changing the random number stored in the random number memory into a predetermined value and storing the changed value in the random number storing portion, and a display for displaying the processed results of the terminal and the server. The server includes a secret key memory for storing a secret key and a random number, a second password generator for generating a one-time password, a second random number changer for storing a random number value identical to the random number value of the terminal, a password receiver for receiving the one-time password of the terminal, a password verifier for

verifying the password to authenticate the user. As a result, it is possible to raise the security level by using a one-time password in which a different password is used each time a user is authenticated, and to save costs by generating a one-time password for various services with a single terminal.

The patent of Asghari-Kamrani et al (application 09/940,635) is solving the identification and authentication issues at the e-commerce level (*"Authentication Problem 2"*). Our invention does not require user/customer to install any hardware device like IC card for authentication.

IN COMPARISON WITH ANANDA, MOHAN ET AL (US-6,385,731 B2)

The patent of Ananda et al, is a secure online PC postage metering system. It's a system for providing secure access and execution of application software stored on a first computer by a second computer using a communication device while a communication link is maintained between the first and second computers. Basically, it is a secure software rental system and not an authentication system.

The patent of Asghari-Kamrani et al (application 09/940,635)) is solving the identification and authentication issues at the e-commerce level (*"Authentication Problem 2"*) and is not for execution of applications stored on a first computer by a second computer.

SUMMARY

In short, our invention:

1. Is intended to solve "**Authentication Problem 2**"
2. Is not a password-based and challenge/response-based authentication system, nor is it a hardware-based or digital certificate-based authentication system
3. Is suited for e-commerce
4. Does not require the user to install any software or hardware
5. Does not require to store any KEY in user's device